

У роботі представлені дослідження комп'ютерних інтернет-мереж на основі концепції статистичної фізики складних мереж, запропоновано метод ймовірнісного моделювання з використанням апарату теорії графів, результати якого узгоджуються з емпіричними даними. Запропонований метод моделювання використаний для розв'язання задачі про стійкість безмасштабних комп'ютерних мереж до спрямованих хакерських атак і розповсюдження комп'ютерних вірусів

Ключові слова: комп'ютерні мережі, стохастичний граф, статистичне моделювання, спрямовані атаки, модель безпеки

В работе представлены исследования компьютерных интернет-сетей на основе концепции статистической физики сложных сетей, предложен метод вероятностного моделирования с использованием аппарата теории графов, результаты которого согласуются с эмпирическими данными. Предложенный метод моделирования использован для решения задачи об устойчивости безмасштабных компьютерных сетей к направленным хакерским атакам и распространению компьютерных вирусов

Ключевые слова: компьютерные сети, стохастический граф, статистическое моделирование, направленные атаки, модель безопасности

УДК 004.942

МОДЕЛЮВАННЯ РОЗВИТКУ СТРУКТУР КОМП'ЮТЕРНИХ МЕРЕЖ

Н. М. Іванущак

Асистент*

E-mail: ivanuschak@yandex.ru

В. В. Пасічник

Доктор технічних наук, професор*

E-mail: vpasichnyk@gmail.com

*Кафедра комп'ютерних систем та мереж
Чернівецький національний університет
імені Юрія Федьковича
вул. Коцюбинського, 2, м. Чернівці,
Україна, 58000

1. Вступ

Метою даної роботи є вирішення задачі, що виникає при створенні нових методів математичного моделювання для дослідження і обґрунтування підходів, які дозволяють ідентифікувати структуру та параметри моделей комп'ютерних мереж з використанням даних спостережень та теорії комплексних мереж.

Для сучасних складних систем характерна нерегулярність зв'язків і висока чисельність елементів, яка може досягати десятків і сотень тисяч. Таким системам та їх мережевим моделям, які володіють нетривіальними топологічними властивостями, найбільшою мірою відповідає термін «комплексні». Комплексною мережею вважається система, яка (а) складається з великої кількості компонентів, (б) допускає «далекосяжні» зв'язки між компонентами; (в) володіє великомасштабною (у тому числі просторово-часовою) мінливістю. Дана мережа є графом з досить великою кількістю вузлів різної природи, що характеризуються багатомірним коротежем ознак і динамічно мінливими зв'язками; розподіл ознак вузлів і характеристик зв'язків може бути описаний ймовірнісною моделлю (багатомірним розподілом).

Основною причиною підвищення актуальності розробок в області теорії і практики комплексних мереж є результати сучасних досліджень реальних комп'ютерних, біологічних і соціальних мереж. Властивості багатьох реальних мереж істотно відрізняються від властивостей класичних випадкових графів з рівноймовірними зв'язками між вузлами, які до недавнього часу розглядалися в якості їх базисного математичного модельного прототипу, і тому побудову їх моделей було запропоновано здійснювати [1,2]

з використанням зв'язних структур і степеневих розподілів.

У теорії комплексних мереж виділяють три основні напрямки:

- дослідження статистичних властивостей, які характеризують поведінку мереж;
- створення моделей мереж;
- прогнозування поведінки при зміні структурних властивостей мереж.

Комплексні мережі використовуються для моделювання об'єктів і систем, дослідження яких іншими способами (за допомогою спостереження або активного експерименту) недоцільні або неможливі.

2. Постановка проблеми

Розуміння структури локальної комп'ютерної мережі впливає з дослідження її еволюції в часі, топології і реального розташування. Локальні мережі створюються для оперування у відносно невеликому географічному просторі. Вони дозволяють множинний доступ до високошвидкісного середовища та управління на основі локального адміністрування.

Комп'ютерні мережі відносяться до мереж, які постійно ростуть і розвиваються. Серед факторів, що впливають на ріст мережі в першу чергу необхідно відзначити розмір або протяжність локальної мережі, яка визначається відстанню між найбільш віддаленими станціями, при якій в нормальному режимі роботи вузлів чітко розпізнаються колізії, і кількість об'єднаних у мережу комп'ютерів. Для Інтернет-мереж цей розмір називається діаметром мережі і складає приблизно 1 км відстані, що дозволяє отримати високу

швидкість зв'язку та максимально можливий рівень сервісу. При зростанні мережі збільшується кількість колізій, різко падає її корисна пропускна здатність і швидкість передачі сигналу. Обмеження мережі за довжиною є передумовою вибору структури мережі, розбиття її на окремі частини (сегменти), появи додаткових серверів з новою мережею зв'язків. Спостерігається динаміка росту мережі, своєрідна кластеризація, сервери виступають центрами утворених кластерів, відбувається просторове позиціонування компонент мережі у вигляді чітких ієрархічних структур.

Мережа розглядається як множина сегментів, кожен з яких закінчується точкою розгалуження або кінцевою вершиною мережі. Вершинами мережі є сервери, комутатори і кінцеві користувачі, загальну кількість яких позначимо N .

Локальні комп'ютерні мережі є об'єктами прототипами графових структур і тому для їх дослідження застосовуються методи теорії графів.

3. Аналіз останніх досліджень та публікацій за темою

Моделювання мереж з використанням апарату теорії графів є важливим напрямком досліджень дискретної математики [3]. В останні роки зросла зацікавленість дослідників до складних мереж з великою кількістю вузлів, зокрема до комп'ютерних мереж, структура яких нерегулярна, складна і динамічно розвивається в часі [4]. Для таких мереж доводиться генерувати стохастичні графи з величезною кількістю вершин. У загальному вигляді модель комп'ютерної мережі являє собою випадковий граф, закон взаємного розміщення ребер і вершин для якого задається розподілом ймовірностей.

В даний час сформульовано чотири основних підходи до моделювання складних мереж:

- випадкові Пуассонівські графи та узагальнені випадкові графи [5];
- Марковські випадкові графи і модель блукання по «графові графів» з ймовірностями, які пропорційні бажаним властивостям [6];
- модель «тісного світу» Ватса і Строгатса [7] і її узагальнення, еволюційна модель росту мережі Барабаші і Альберт [1,2];
- модель Прайса [8].

Перші три підходи передбачають генерацію випадкового графа із заздалегідь відомою кількістю вершин і заданими ймовірнісними властивостями.

Більшість реальних графів підпорядковуються степеневому закону розподілу $P(k)$. Ці графи побудови мереж описуються моделлю переважного приєднання Барабаші-Альберт [1,2]. Через далекосяжні взаємодії у системи не існує масштабу зміни характерних величин. Ріст і переважне приєднання є основними механізмами побудови безмасштабних мереж.

Нехай вузол i має k_i зв'язків і він може бути приєднаним (зв'язаним) до інших вузлів k_i . Ймовірність приєднання нового вузла до вузла i залежить від ступеня k_i вузла i . Величина $W(k_i) = \frac{k_i}{\sum_j k_j}$ називається

переважним приєднанням (preferential attachment). Не всі вузли мають однакову кількість зв'язків, тому

вони характеризуються функцією розподілу $P(k)$, що визначає ймовірність того, що випадково вибраний вузол має k зв'язків. Для комплексних мереж функція $P(k)$ відрізняється від розподілу Пуассона для випадкових графів. Для переважної більшості комплексних мереж, до яких відносяться досліджувані локальні комп'ютерні мережі, спостерігається степенева залежність $P(k) \sim k^{-\gamma}$.

4. Ймовірнісна модель комп'ютерної мережі

Комп'ютерна мережа зображується у вигляді графа G , який визначається як сукупність (V, E) кінцевої множини вершин V , $\dim(V) = N$, і множини ребер E , яка складається із неупорядкованих пар (u, v) де $u, v \in V$ і $u \neq v$.

Кожна вершина характеризується своїм ступенем, тобто числом інцидентних їй ребер. Впорядкований список ступенів вершин називається ступеневою послідовністю.

Інтегральною характеристикою комп'ютерної мережі є закон розподілу ступенів p_k , який задає ймовірність того, що випадково вибрана вершина має ступінь k . Ступеневу послідовність для неорієнтованого графа зручно подати у формі

$$d = (k_1^{n_1}, k_2^{n_2}, \dots, k_s^{n_s}),$$

де числа k_i є ступенями вершин, а показник n_i визначає кількість повторів числа k_i у послідовності. Так, наприклад $(3^1, 2^2, 1^4) = (3, 2, 2, 1, 1, 1)$. Такий запис дозволяє пов'язати дискретний розподіл ступенів вершин p_k зі ступеневою послідовністю d у формі

$$p_k \stackrel{\text{def}}{=} P[x = k_i] = n_i / N.$$

У загальному випадку степенева послідовність є монотонною незростаючою, однак у випадку генерації комп'ютерних мереж дана вимога не є обов'язковою.

У моделі випадкових графів [5] ребро, яке інцидентне довільним двом вершинам, присутнє або відсутнє з рівною ймовірністю, а тому розподіл p_k є біноміальним або (у границі за N) Пуассонівським. Однак більшість реальних мереж має структуру відмінну від структури випадкових графів, що позначається на характері розподілу ступенів вершин. Зокрема, у багатьох реальних мережах емпіричний розподіл ступенів вершин інтерпретується в термінах ступеневого розподілу $p_k = k^{-\gamma} / \zeta(\gamma)$, де ζ - функція Рімана відіграє роль нормуючої константи. Цей розподіл характеризується єдиним параметром γ , який визначає швидкість спадання «хвоста» розподілу.

Для здійснення процесу моделювання комп'ютерних інтернет-мереж використовувались характеристики реальних мереж «BV-Star & FoxNet», «KTM» та «DSS-Group» у м. Чернівцях, наведені в табл. 1.

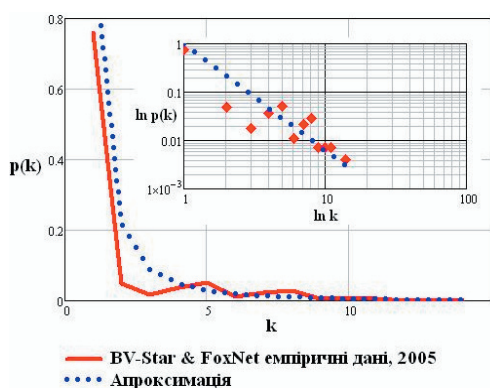
В процесі досліджень ми мали можливість простежити за розвитком та структуризацією комп'ютерної мережі «BV-Star & Fox Net» в часі. Характеристики цієї мережі в різні часові проміжки наведені в табл. 1. Якщо на початку становлення мережа займала проміжне

місце між масштабною з Пуассонівським розподілом ступенів вершин та безмасштабною мережами, то з часом відбувається ріст та структуризація системи, розподіл ступенів вершин для неї вже інтерпретується в термінах степеневого розподілу $p_k = k^{-\gamma}$, причому значення показника $\gamma = 2,4$ практично залишається незмінним за останні роки в період з 2008 по 2011 рік, що вказує на те, що топологічні властивості мережі спрямувались до стійкого стаціонарного стану.

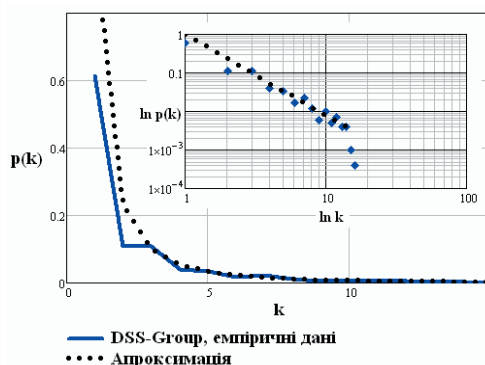
Таблиця 1

Характеристики комп'ютерних мереж

	«BV Star & Fox Net » у м. Чернівцях						«KTM» у м.Чернів- цях		«DSS- Group» у м.Чернів- цях	
	2005		2008		2011					
	N=272		N=588		N=915					
k	n _k	p _k	n _k	p _k	n _k	p _k	n _k	p _k	n _k	p _k
1	207	0.761	401	0.682	614	0.671	1214	0.756	1242	0.613
2	13	0.048	37	0.063	59	0.064	67	0.042	224	0.110
3	5	0.018	48	0.082	79	0.086	71	0.044	220	0.110
4	10	0.036	28	0.047	51	0.056	38	0.024	79	0.040
5	14	0.051	19	0.032	22	0.024	84	0.052	68	0.033
6	3	0.011	14	0.024	33	0.036	34	0.021	35	0.017
7	6	0.022	6	0.010	9	0.010	20	0.012	46	0.022
8	8	0.029	8	0.014	8	0.009	26	0.016	26	0.012
9	2	0.007	8	0.014	10	0.011	7	0.004	13	0.006
10	2	0.007	6	0.010	6	0.006	15	0.009	21	0.010
11	2	0.007	6	0.010	8	0.009	3	0.002	10	0.005
12	0	0	2	0.003	7	0.008	13	0.008	14	0.007
13	0	0	2	0.003	3	0.003	4	0.002	8	0.004
14	1	0.004	1	0.001	3	0.003	2	0.001	9	0.004
15	0	0	2	0.003	3	0.003	4	0.002	4	0.002



а)



б)

Рис. 1. Апроксимація «хвостів» розподілів ступенів вершин досліджуваних мереж:
а) «BV-Star & FoxNet»; б) «DSS-Group»

Отже, якщо мережа достатньо структуризована, то в процесі її розвитку змінюється кількість вершин n_k із заданим ступенем приєднання вузла k , рівно як і загальна кількість N користувачів мережі, однак ймовірності приєднання цих вершин p_k залишаються практично незмінними, забезпечуючи тим самим степеневий розподіл ступенів вершини $p_k = k^{-\gamma}$ з незмінним показником γ .

5. Спосіб генерації комп'ютерної мережі для заданого закону розподілу ступенів вершин

Параметри узагальненої конфігураційної моделі:

N – число вершин у мережі;

s – число класів вершин;

$i \in \{1, 2, 3, \dots, s\}$ – позначає конкретний клас вершин;

n_i – число вершин i -го класу;

k_i – ступінь вершини i .

Так як розподіл ступенів вершин p_k заданий, то зведемо обчислювальну процедуру до наступних операцій:

- сформуємо ступеневу послідовність d , вибираючи s чисел n_i згідно із заданим розподілом p_k , де $i = 1, s$;

- кожній вершині i графа присвоїмо k_i «заготовок» (кінців) для майбутніх ребер;

- зі ступеневої послідовності випадково отримуються пари «заготовок». Вони з'єднуються ребром у тому випадку, якщо нове ребро не приведе до утворення ребер-циклів (петель) або мультиребер. Якщо ребро згенероване, то відповідні індекси із ступеневої послідовності видаляються;

- попередній крок повторюється до тих пір, поки ступенева послідовність не стане порожньою;

- укладка графа здійснюється шляхом розміщення вершин з найбільшими ступенями приєднання в центрі графа, а вершини з меншими ступенями радіально розташовуються від центру до периферії в порядку зменшення їх ступенів;

- зв'язки між вузлами заповнюються послідовно, починаючи з вершин з найбільшою кількістю ребер.

Остання умова забезпечує об'єднання всіх вузлів у єдину структуру стохастичного графа, що відображає факт обов'язкового приєднання всіх користувачів у реальну локальну комп'ютерну мережу.

На основі розподілу p_k довільний граф може бути побудований $\prod k_i!$ різ-

ними способами, так як «заготовки» для майбутніх ребер нерозрізними. Таким чином, цей процес з рівною ймовірністю генерує довільну можливу конфігурацію мережі із заданим розподілом ступенів вершин p_k .

Перевагою даного алгоритму є його універсальність, так як з його допомогою можливо побудувати мережу з довільним розподілом ступенів вершин.

6. Комп'ютерний експеримент

Результатом програмної реалізації запропонованого алгоритму є власне комп'ютерна мережа, зображена у вигляді стохастичного графа з відомим числом вершин і заданим розподілом ймовірностей їх приєднання.

Робота алгоритму моделювання, адекватність описання моделлю реальної структури проілюстрована шляхом генерації графа з використанням характеристик реальних комп'ютерних мереж BV-Star & Fox Net та DSS-Group в м. Чернівцях. За вибіркою визначено розподіли таких числових характеристик для реальних мереж:

1) кількість вершин у мережі n_k з різними ступенями їх приєднання;

2) впорядкований список ступенів вершин у вигляді ступеневої послідовності $d = (k_1^{n_1}, k_2^{n_2}, \dots, k_s^{n_s})$ для моделювання стохастичного графа;

3) відповідні ймовірності $p_1, p_2, p_3, \dots, p_s$ приєднання вершин з різними ступенями k_i ($i=1, s$) у мережу.

Вибірка здійснювалася за емпіричними розподілами ступенів вершин, які інтерпретуються в термінах степеневого розподілу $p_k = k^{-\gamma}$, на її основі здійснений процес моделювання мережі з подальшою можливістю порівняння результатів моделювання з характеристиками досліджуваних мереж, наведеними у табл. 1, та оцінювання адекватності описання моделлю реальної структури.

Провівши апроксимацію «хвостів» розподілів ступенів вершин, що проілюстровано на рис.1, та визначивши тим самим показники γ для різних локальних комп'ютерних мереж, зокрема $\gamma=2,4$ для мережі «BV-Star & Fox Net», $\gamma=2,6$ для мережі «КТМ» та $\gamma=2,1$ для мережі «DSS-Group», здійснено моделювання цих мереж за відомим степеневим $p_k = k^{-\gamma}$ розподілом ймовірностей приєднання користувачів у мережу з відповідними γ .

Як ілюстрація на рис. 2 наведені приклади візуалізації стохастичних графів, які зображають структурні властивості досліджуваних комп'ютерних мереж.

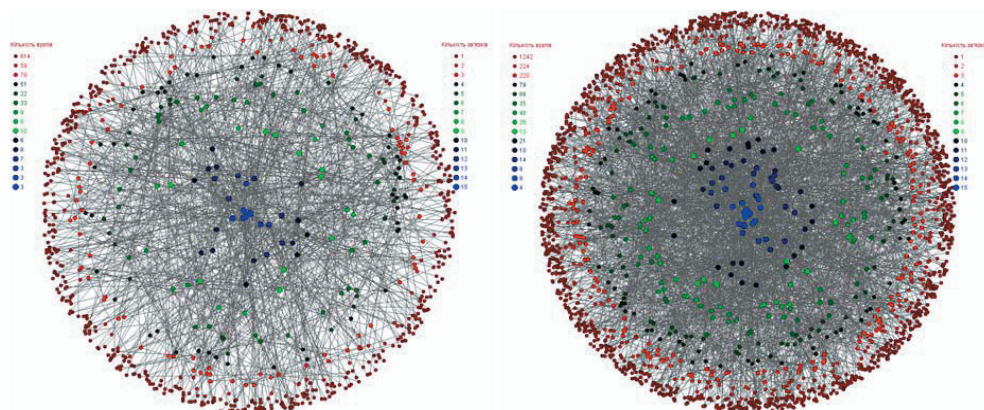


Рис. 2. Приклади графів, які відповідають мережам з різними законами залежності $p_k = k^{-\gamma}$: (а) $\gamma=2,4$, $N=915$; (б) $\gamma=2,1$, $N=2023$

Для здійснення процесу динамічної візуалізації використовувався алгоритм укладання графа, який, на нашу думку, дає найбільш інформативне відображення структури та властивостей комп'ютерних мереж. У центрі графа розміщуються вершини з найвищим ступенем вершин, навколо яких послідовно розташовуються вершини з нижчими ступенями приєднання вузлів.

Наступним кроком є генерація ребер E , тобто процес випадкового з'єднання пар заготовок вершин. При цьому відслідковуються утворення нових ребер, щоби у графі не з'явилися мультиребра. Алгоритм реалізований у середовищі Processing із загальнодоступною мовою програмування і високоякісною візуалізацією зображень.

На рис. 2 вершини з різними ступенями приєднання k зображені різними кольорами, їх кількість у згенерованій мережі винесено на панель зліва, кількість зв'язків, які відповідають кожній вершині, відображені на панелі справа. Для малих значень параметра розподілу γ мережа кластеризується в один більший зв'язаний кластер, а ніж у випадку з більшими значеннями γ .

Завдяки тому, що основний внесок у мережу роблять користувачі, для яких ступінь приєднання у мережу $k=1$, то середній ступінь мережі $\langle k \rangle = \sum_k k \cdot p_k$, знайдений у такий спосіб, є порівняно малою величиною. Для мережі «BV-Star & Fox Net» його значення $\langle k \rangle = 1,997$. Слід відмітити, що для переважної більшості комп'ютерних Інтернет-мереж середній ступінь $\langle k \rangle$ в силу тих же причин прийматиме малі значення.

Щодо параметра γ показника степеня степеневого розподілу, то його значення може бути різним. Більшим – у менш розгалужених системах з порівняно малою кількістю серверів, комутаторів з багатьма зв'язками k і навпаки великою кількістю користувачів з $k=1$. Меншим – у більш структуризованих мережах, у структурі яких є достатня кількість вершин з великими ступенями k (рис. 2б), таких як мережа DSS-Group у м. Чернівцях.

Запропонований у роботі алгоритм дозволяє здійснити прогнозування розвитку мережі. Як приклад, відслідковуючи динаміку становлення мережі «BV-Star & Fox Net» за останні роки, наведену в табл. 1, здійснивши процес моделювання за визначеним для неї інтегральним законом розподілу ймовірностей $p_k = k^{-2.4}$ та щорічним приростом $\Delta N \approx 110$ вершин цієї мережі, можна обчислити прогнозовану кількість користувачів, серверів та комутаторів у ній у 2014 р. (табл. 2).

Таблиця 2

Прогнозована кількість зв'язків у мережі
«BV-Star & Fox Net»

N= =1245	k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	n_k	751	271	89	45	26	17	12	8	6	5	4	3	3	3	2

У роботі питання про адекватність моделі встановлюється через зіставлення оцінок апроксимованого усередненого та реального розподілів ступенів вузлів p_k згідно з формулою $\sigma^2 = \frac{1}{n} \sum_{k=1}^n (p_k - \bar{p}_k)^2$. Розкид даних для досліджуваних мереж у різні часові проміжки, наведених у табл. 1, порівняно з усередненими апроксимованими у відсотковому відношенні складає $7.5 \pm 3.5\%$ мінливості варіаційного ряду, що свідчить про адекватність описання моделлю реальних мереж.

7. Визначення оптимальної стратегії захисту локальних мереж від спрямованих атак

Алгоритми моделювання, запропоновані в роботі, стали засобом для вироблення підходів до оцінювання процесів розповсюдження вірусів у комп'ютерних мережах та дослідження їх уразливості та стійкості до спрямованих атак.

Аналіз реальних безмасштабних мереж WWW та Інтернету [9,10], метаболізму [11] та мереж харчування [12] демонструє неабияку їх стійкість до вилучення вузлів: тобто ці мережі виявляють несподіваний ступінь стійкості при випадкових ураженнях. З іншого боку, при спланованих сценаріях нанесення шкоди або вірусних атаках, мережа стає надзвичайно уразливою.

Випадковим атакам (відмова, збоєм, R-атакам) властивий випадковий вибір атакуючого вузла. Класична стратегія цілеспрямованих атак (I-атак) полягає у послідовному знищенні вузлів з максимальною зв'язністю. Зазвичай наслідки атак досліджуваних мереж аналізуються з допомогою широкого набору метрик: реєструються зміни діаметра, коефіцієнта кластерності, розміру максимального кластера і його відносних величин. В реальному житті спостерігається більш складні ситуації, тобто вузли і зв'язки комп'ютерних мереж різної топології, що володіють різною уразливістю, піддаються неоднорідним випадковим і цілеспрямованим загрозам, причому в різноманітних комбінаціях.

Розроблена узагальнена агентна модель еволюції мережевого ансамблю в умовах дестабілізуючих загроз. Основними компонентами описової конструкції мережі являються *модель загроз* та *модель безпеки* [13].

На вхід *моделі загроз* подається сформований стохастичний граф, що відображає структуру реальної мережі. Над графом проводяться два сценарії атак – «природна» ліквідація вершин і ребер, що відповідає випадковим R-атакам та ліквідація вершин з найбільшими ступенями, тобто I-атака. Відносний розмір максимального кластера S визначається часткою вузлів, що містяться у найбільшому кластері мережі:

$$S = 1 - \sum_{k=1}^{k_{\max}} \frac{k \cdot n_{\text{del}}(k)}{N},$$

де $n_{\text{del}}(k)$ – кількість видалених вузлів ступеня k , N – загальна кількість вузлів у мережі.

Розвиток даної моделі дозволяє здійснити імітацію атак у вигляді комбінованих загроз (R-випадкової та I-цілеспрямованої) незахищеним вузлам мережі в прямій (R-загрози + I-загрози) та зворотній (I-загрози + R-загрози) послідовності.

На рис. 3 представлені результати зміни відносного розміру максимального кластера в залежності від числа атакуючих вузлів безмасштабних комп'ютерних мереж «BV-Star & FoxNet» та «DSS-Group» м. Чернівці. Видно, що для будь-якої з представлених мереж атакуюча комбінація I-R є більш ефективною, ніж R-I.

Модель безпеки [13] враховує, що основною мірою безпеки є ризик:

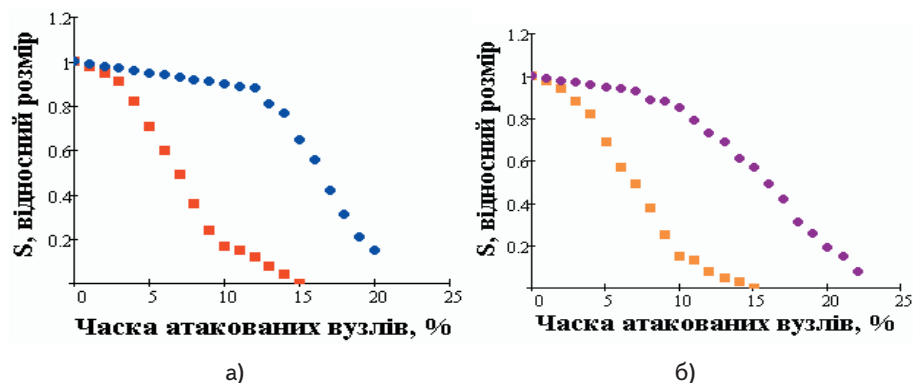


Рис. 3. Залежність відносного розміру максимального кластера в мережах «BV-Star & FoxNet» (а) та «DSS-Group» (б) від кількості атакуючих вузлів, що піддаються атакам у різній послідовності: I+R (■) та R+I (●)

$$R = \rho_{\text{th}} \cdot \rho_v \cdot Pl,$$

де R – ризик, ρ_{th} і ρ_v – відповідні ймовірності загрози та уразливості, Pl – ціна втрати.

Модель дозволяє шляхом співставлення опису джерел загроз, близьких до реальних, вивчати більш складні атаки на системи, ніж у їх традиційному трактуванні для теорії комплексних мереж. Даний підхід дає можливість для кожного вузла ввести параметр уразливості (або захищеності), на відміну від багатьох відомих, де наслідком атаки завжди є знищення вузла чи зв'язка. Елементам мережі приписуються величини їх уразливості, в загальному випадку, з $\rho_v(i)$ відмінними від 1, які визначаються об'ємом фінансових вкладів F_i в безпеку i -го елемента:

$$\rho_v(i) = f(F_i).$$

Ціна втрати – як реакція мережі на атаку – визначається вибором елемента із множини метрик M – тих індикаторів працездатності, які визначають головні цільові характеристики мережевих ансамблів. Наприклад, в якості елементів множини M можуть використовуватися значення коефіцієнта кластерності, посередництва, максимальний розмір кластера, найкоротші шляхи тощо.

Для комп'ютерних мереж «BV-Star & FoxNet», «КТМ» та «DSS-Group» досліджувалась реакція відповідних змодельованих стохастичних графів на цілеспрямовані загрози захищених елементів – вузлів. Вважалось, що ймовірність успішної атаки на вузол змінюється тільки зі зміною $\rho_v(i)$, яка експоненційно

зменшується зі збільшенням «товщини» захисного бар'єра d_i , який в свою чергу визначається традиційним комплексом заходів безпеки: правовими, організаційними, технічними, фізичними і математичними. Величина d_i визначається об'ємом затрат, тобто $d_i \sim F_i$, і в такому випадку:

$$\rho_v(i) \sim \exp(-\mu F_i),$$

де μ – коефіцієнт, який задає ефективність використання фінансових затрат.

На практиці різні елементи мережі – вузли і зв'язки – захищені (фінансуються) по-різному. Так, зазвичай найбільш важливі агенти мережі захищаються більшою мірою.

Вважаючи, що стратегія безпеки визначає розподіл ресурсів між вузлами, здійснене дослідження реакції мережі на загрози для випадків відсутності фінансування та трьох можливих стратегій розподілу інвестицій для захисту, які залежать від ступеня вузла (при однаковому сумарному об'ємі):

- відсутність інвестицій $F_0 = 0$;
- низька захищеність усіх вузлів мережі $F_1 = 1/\mu$;
- середня захищеність вузлів з високими та середніми ступенями $F_2 = 4.1k_i/\mu$;
- максимальний рівень захисту вузлів з високими ступенями $F_3 = 28k_i^2/\mu$.

$$\sum_{i=1}^{1000} F_1 = \sum_{i=1}^{1000} F_2 = \sum_{i=1}^{1000} F_3.$$

Для тестової мережі, що містить 1000 вершин, використовувалася класична стратегія цілеспрямованих атак з послідовними атаками на вузли максимального ступеня.

Результати розрахунків зміни відносного розміру максимального кластера для цих чотирьох варіантів захисної стратегії наведені на рис. 4.

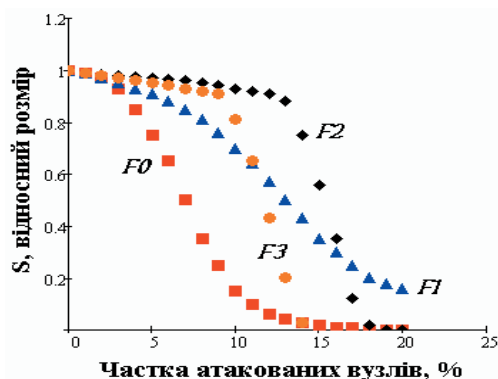


Рис. 4. Залежність відносного розміру максимального кластера в мережі від кількості атакованих вузлів при різних захисних стратегіях розподілу інвестицій: $F_0 = 0$, $F_1 = 1/\mu$, $F_2 = 4.1k_i/\mu$, $F_3 = 28k_i^2/\mu$

Видно, що стратегія надмірного захисту вузлів максимальної зв'язаності (тобто $F_1 \sim k_i^2$) не є оптимальною. Таку поведінку можна пояснити тим, що на захист елементів меншого ступеня просто не вистачає коштів.

Будуючи оптимальну стратегію захисту мережі, обумовлену як вибором її топології, так і розподілом ресурсів для захисту її елементів, необхідно максимально точно оцінювати стратегію та дії атакуючої сторони.

Із рис. 4 видно, що оптимальною стратегією захисту локальних комп'ютерних мереж є стратегія захищеності вузлів із високими та середніми ступенями. Тому для вивчення властивостей, пов'язаних з надійністю, захистом від уразливості локальних комп'ютерних мереж, була реалізована процедура виділення «опорної мережі», що полягає у багатоетапному відрізання листів початкового графа (рис. 5).

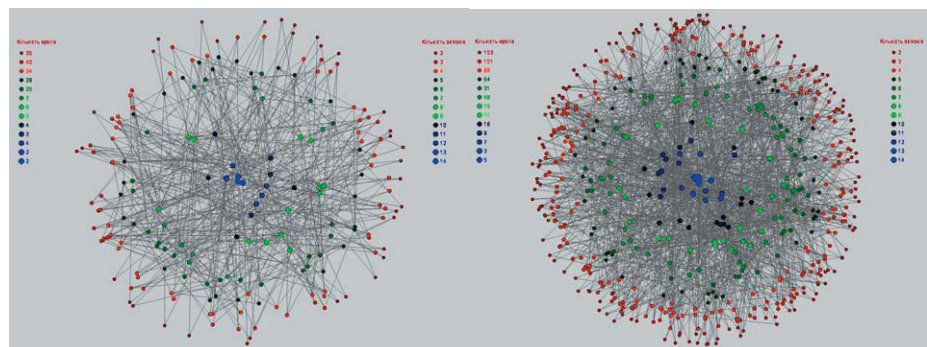


Рис. 5. Опорні мережі Інтернет провайдерів «BV-Star & FoxNet» та «DSS-Group»

Розглянуті опорні мережі виявилися безмасштабними, залежність розподілу ступенів їх вузлів з високою точністю апроксимується степеневою функцією. Вивчені і представлені нові наближені до реальності приклади поведінки комп'ютерних мереж у полі загроз, які дозволяють ефективно підійти до рішення широкого спектра задач стійкості практично значущих мережевих конструкцій.

8. Висновки

Обчислені інтегральні ймовірнісні характеристики реальних комп'ютерних мереж Інтернет-провайдерів м. Чернівці: «BV-Star & FoxNet», «Кабельне телебачення міста» та «DSS-Group» у різні часові проміжки, проведена їх апроксимація для здійснення процесу моделювання.

Розроблений метод генерування структури локальних комп'ютерних мереж із заданою функцією щільності розподілу ступенів вузлів з використанням апарату теорії складних мереж, що дозволяє відтворювати ці мережі як стохастичний граф із заданими ймовірнісними властивостями. На основі запропонованого у роботі алгоритму моделювання здійснене прогнозування еволюційної динаміки розвитку та становлення реальних комп'ютерних мереж на наступні роки.

Запропонований в роботі метод використаний для оцінювання уразливості змодельованих безмасштабних комп'ютерних мереж та розв'язана задача про стійкість до випадкових та спрямованих атак. Розроблена узагальнена модель еволюції мережевого ансамблю в умовах дестабілізуючих загроз.

Література

1. Albert, R. Statistical mechanics of complex networks [Text] / R. Albert, A.-L. Barabasi // Reviews of Modern Physics. – 2002. – P. 47-97.
2. Barabasi, A.-L. Emergence of scaling in random networks [Text] / A.-L. Barabasi, R. Albert // Science. – 1999. – Vol. 286. – P. 509-512.
3. Нікольський, Ю. Дискретна математика [Текст] / Ю.В. Нікольський, В.В. Пасічник, Ю.М. Щербина // Львів: «Магнолія – 2006». – 2009. – 432 с.
4. Newman, M.E.J. The Structure and Function of Complex Networks [Text] / M.E.J. Newman // SIAM Review. – 2003. – Vol. 45. - N. 2. – P. 167-256.
5. Erdős, P. On the evolution of random graphs [Text] / P. Erdős, A. Renyi // Publications of the Mathematical Institute of the Hungarian Academy of Sciences. – 1960. – Vol. 5. – P. 17-61.
6. Frank, O. Markov graphs [Text] / O. Frank, D. Strauss // Journal of the American Statistical Association. – 1986. – Vol. 81. – P. 832-842.
7. Watts, D.J. Collective dynamics of “small-world” networks [Text] / D.J. Watts, S.H. Strogatz // Nature. – 1998. – Vol. 393. – P. 440-442.
8. Price, D.J. de S. A general theory of bibliometric and other cumulative advantage processes [Text] / D.J. de S. Price // Journal of the American Society for Information Science. – 1976. – Vol. 27. – P. 292-306.
9. Albert, R. Error and attack tolerance of complex networks [Text] / R. Albert, H. Jeong, A.-L. Barabasi // Nature (London). – 2000. – Vol. 406. – P. 378 – 381.
10. Tu, Y. How robust is the Internet? [Text] / Y. Tu // Nature (London). – 2000. – Vol. 406. – P. 353 – 354.
11. Jeong, H. The large-scale organization of metabolic networks [Text] / H. Jeong, B. Tombor, R. Albert, Z. N. Oltvai, A.-L. Barabasi // Nature (London). – 2000. – Vol. 407. – P. 651 – 654.
12. Sole, R. V. Complexity and fragility in ecological networks [Text] / R.V. Sole, J.M. Montoya // Proc. R. Soc. Lond. – 2001. – B 268. – P. 2039 – 2045.
13. Galindo F. Modeling of Aggregate Attacks on Complex Networks / F. Galindo, V.Dmitrienko, A.Caruso, A. Rossodivita, A.A.Tikhomirov, A. I.Trufanov, E. V. Shubnikov // Information Security Technologies, Moscow – 2010. - N3. - P.115-121.

Розглядається питання створення інформаційно-аналітичних систем для задач охорони здоров'я, зокрема для задачі визначення чисельності груп ризику інфікування ВІЛ/СНІДу; визначено принципи побудови СППР та її складові; проведено аналіз задач, які виникають при розробці інформаційно-аналітичних систем для задач охорони здоров'я

Ключові слова: інформаційно-аналітичні системи, групи ризику інфікування ВІЛ/Сніду, принципи побудови ІАС

Рассматривается вопрос создания информационно-аналитических систем для задач здравоохранения, в том числе для задачи определения численности групп риска инфицирования ВИЧ/СПИДа; определены принципы построения СППР и ее составляющие; проведен анализ задач, которые возникают при разработке информационно-аналитических систем для задач здравоохранения

Ключевые слова: информационно-аналитические системы, группы риска инфицирования ВИЧ/СПИДа, принципы построения ИАС

УДК 004.896+519.816

АНАЛІЗ ІНФОРМАЦІЙНОЇ ТЕХНОЛОГІЇ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ДЛЯ ЗАДАЧІ ОХОРОНИ ЗДОРОВ'Я

О. Ю. Мулеса

Старший викладач

Кафедра кібернетики і прикладної математики

Ужгородський національний університет

вул. Університетська, 14, м. Ужгород, Україна,

88000

E-mail: mulesa.oksana@gmail.com

1. Вступ

Широке впровадження інформаційних технологій в різні галузі науки, техніки, народного господарства стало наслідком значного збільшення обсягу

інформації, необхідної для аналізу та обробки в наукових дослідженнях та різних прикладних галузях. Виклики, які повсякчас виникають перед дослідниками в різних науково-прикладних напрямках, як правило не можуть бути вирішеними без застосуван-